No. 98591-0

IN THE SUPREME COURT
OF THE STATE OF WASHINGTON

STATE OF WASHINGTON,
Petitioner,
v.
LYNELL AVERY DENHAM,
Respondent.

BRIEF OF *AMICI CURIAE* WASHINGTON ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON, KING COUNTY DEPARTMENT OF PUBLIC DEFENSE, AND WASHINGTON DEFENDER ASSOCIATION

[*Counsel Listed on Following Page*]

John R. Tyler, WSBA #42097
Anna Mouw Thompson, WSBA #52418
Rachel Dallal, WSBA #88558
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000
RTyler@perkinscoie.com
AnnaThompson@perkinscoie.com
RDallal@perkinscoie.com

Counsel for Amicus Curiae Washington Association of Criminal Defense Lawyers

La Rond Baker, WSBA #43610
Katie Hurley, WSBA #37863
Brian Flaherty, WSBA #41198
KING COUNTY DEPARTMENT OF PUBLIC DEFENSE
710 Second Avenue, Suite 250
Seattle, WA 98104
Phone: (206)263-6884
lbaker@kingcounty.gov
Katherine.hurley@kingcounty.gov
Brian.flaherty@kingcounty.gov

Mark B. Middaugh, WSBA #51425
WACDL AMICUS COMMITTEE
1511 Third Avenue, Suite 503
Seattle, WA 98118
(206) 919-4269
Mark.middaugh@gmail.com

Antoinette M. Davis, WSBA #29821
Nancy Talner, WSBA #11196
ACLU OF WASHINGTON FOUNDATION
P.O. Box 2728
Seattle, WA 98111
(206) 624-2184
Tdavis@aclu-wa.org
Talner@aclu-wa.org

Alexandria "Ali" Hohman, WSBA #44104
Director of Legal Services
WASHINGTON DEFENDER ASSOCIATION
110 Prefontaine Pl S # 610
Seattle, WA 98104
Ph: 206- 623-4321
ali@defensenet.org

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(continued)

Page(s)

IDENTITY AND INTEREST OF AMICI

The identity and interest of Amici are set forth in the Motion for Leave to File Brief of Amici Curiae filed with this brief.

ISSUES TO BE ADDRESSED BY AMICI

First, whether the nexus requirement means that a warrant to search cell phone or cell-site location information ("CSLI") records must be based on specific facts that show probable cause to believe evidence of the crime under investigation will be found in those particular records, rather than on generalized statements regarding the prevalence of cell-phone use; and

Second, whether the "scrupulous exactitude" standard should apply when law enforcement seeks to search cell phone and CSLI records because such materials raise unique First Amendment concerns.

STATEMENT OF THE CASE

During an investigation into Mr. Denham for a sophisticated jewelry heist, the Washington state police applied for and obtained a search warrant for CSLI. In support, a detective submitted an affidavit establishing that (1) the two cell phone numbers at issue belonged to Mr. Denham; (2) Mr. Dehman used these cell phones to contact buyers for the stolen jewelry, and (3) "the majority of Americans possess and use cellular telephones, and . . . most of those keep the phones within their reach at all times." Opinion at 12. Mr. Denham challenged the sufficiency of the warrant in the trial court, but the court held that the warrant was constitutionally sufficient. The resulting CSLI records were inculpatory.

The State's witnesses at trial testified that the records showed a "hit" off a cellphone tower near the jewelry store during the time of the burglary.

On appeal, the Court of Appeals disagreed. As relevant here, it held that the warrant for CSLI was improvidently granted because "[t]he application for the search warrant for Denham's cell phone records was insufficient as it failed to provide specific information demonstrating a nexus between Denham, the criminal act, the information to be seized and the item to be searched." *Id*. at 13. In particular, the warrant application "failed to establish that Denham had either of the cell phones in question in his possession on the night of the burglary," and instead relied on only "blanket inferences and generalities" about typical cell phone habits to support the assertion that evidence would be found in Mr. Denham's records. In other words, it failed to establish a "nexus between criminal activity and the item to be seized and the place to be searched." *Id*. at 6 (quoting *State v. Goble*, 88 Wn. App 503, 509, 945 P.2d 263 (1997)).

SUMMARY OF ARGUMENT

The Court of Appeals correctly held that the warrant to search Mr. Denham's CSLI was deficient under existing law because the nexus requirement was unmet—namely, because the affidavit did not include specific facts showing probable cause to believe that a search of Mr. Denham's CSLI would uncover evidence of the burglary, theft, and sale of stolen property under investigation. This was no novel holding: It is merely an application of the well-established principle that a search warrant must be based on probable cause to believe that evidence of a crime will be

found in a specific place. Both the Fourth Amendment and article I, section 7 of the Washington Constitution, which is *more* protective than the Fourth Amendment, plainly require as much.

This Court should, however, hold that the relevant standard is even more exacting than that applied by the Court of Appeal. Namely, because cell phone and CSLI records contain expressive materials and reveal a wealth of information about associational activities, they should be presumptively protected by the First Amendment—in which case constitutional protections (like those demanding a nexus, particularity, and sufficient tailoring) are applied with "scrupulous exactitude." Once again, such a holding is especially appropriate because the Washington Constitution provides *greater* protections than the Fourth Amendment.

Finally, the sheer invasiveness of searches involving cell phone and CSLI records shows the importance, in an appropriate case, of providing courts with clear, bright line rules to ensure that application of the scrupulous exactitude standard confers meaningful privacy protections.

ARGUMENT

I. Searches of cell phone data, such as CSLI, are uniquely invasive.

No other data repository rivals the cell phone in terms of the quantity and quality of personal information it holds. Six years ago, the Supreme Court held that cell phones "are in fact minicomputers" capable of replacing "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, [and] newspapers." *Riley v. California*, 573 U.S. 373, 393, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014). That list has

continued to expand exponentially, as cell phones are used in increasingly novel ways. For example, cell phones can now be used to download fitness tracking applications, monitor diabetic patients' glucose levels,[1] pair with devices that take electrocardiograms,[2] and contact-trace to mitigate the ongoing coronavirus pandemic.[3] Due to this technological omnipotence, the search of a single cell phone might reveal a person's "travel history, weight loss goals, religious beliefs, political affiliations, financial investments, shopping habits, romantic interests, medical diagnoses, and on and on." *State v. Fairley*, 12 Wn. App. 2d 315, 323, 457 P.3d 1150 (2020). Even the search of an entire home, a place that is considered "first among equals" under the Fourth Amendment, would expose less personal information than the unfettered search of a cell phone. *Florida. v. Jardines*, 569 U.S. 1, 6, 133 S. Ct. 1409, 185 L. Ed. 2d 495 (2013). The only consistent exception to this rule occurs when the search of a home turns up a cell phone. *See Riley*, 573 U.S. at 396-97 ("A phone . . . contains a broad array of private information never found in a home in any form—***unless the phone is***.") (emphasis added).

---

[1] *See Diabetes Ctrs. of Am., Inc. v. Healthpia Am., Inc.*, Civil Case No. H-06-3457, 2007 WL 2363297, at *1 (S.D. Tex. Aug. 17, 2007) (involving the "GlucoPhone . . . a cell phone that can test and read a patient's glucose levels, store the test results, and transmit the test results to physicians or others designated by the patient").

[2] *See Taking an ECG with the ECG app on Apple Watch Series 4, Series 5, or Series 6*, APPLE, https://support.apple.com/en-us/HT208955 (last visited Dec. 7, 2020), (explaining how to use an "ECG app . . [to] record your heartbeat and rhythm using the electrical heart sensor on Apple Watch . . . and then check the recording for atrial fibrillation (AFib), a form of irregular rhythm").

[3] *See generally* Matt Richtel, *Contact Tracing With Your Phone: It's Easier but There Are Tradeoffs*, N.Y. TIMES (June 3, 2020, updated July 20, 2020), https://www.nytimes.com/2020/06/03/health/coronavirus-contact-tracing-apps.html.

Cell phones can also provide real-time information because operating systems and applications sync continuously through the cloud. This fact also makes cell phone searches unique. For example, if law enforcement seizes a physical day planner, that object will certainly hold a fair amount of personal information—but it will only provide historical information. By contrast, if law enforcement seizes a cell phone, the device might continue to sync calendar entries (along with photos, videos, and location data from "map" applications) even after it has been seized. Thus, the seizure of a cell phone starts to look more like a wiretap than a traditional search. *See* 18 U.S.C. § 2510, *et. seq.* (federal Wiretap Act); Matthew J. Tokson, *The Content/envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2118–19 (2009) (explaining how the federal Wiretap Act requires the government to meet a heightened standard to obtain a "super-warrant" when it seeks to obtain *prospective* communication content); *see also* RCW § 9.73.040 (imposing similar heightened requirements for interception of communications under Washington law).

This case, of course, involves a search of CSLI. Cell phones "continuously scan their environment looking for the best signal, which generally comes from the closest cell site," i.e., the closest radio antennas mounted to nearby towers or other tall structures. *Carpenter v. United States*, 138 S. Ct. 2206, 2211, 201 L. Ed. 2d 507 (2018). "Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI)." *Id*. Those records are held by a wireless carrier in the ordinary course of business, and are often sought by

law enforcement in order to ascertain the location of a suspect at the time of the crime in question. But CSLI raises unique privacy concerns, as succinctly summarized by this very Court:

> Historical and real-time CSLI, like text messages, reveal an intensely intimate picture into our personal lives. Our cell phones accompany us on trips taken to places we would rather keep private, such as 'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.' This type of information, revealed by our public movements, can expose personal details about family, politics, religion, and sexual associations.

State v. Muhammad, 194 Wn.2d 577, 589, 451 P.3d 1060 (2019) (quoting *United States v. Jones*, 565 U.S. 400, 415, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring)). The U.S. Supreme Court has also aptly noted that location information created by cell phones is uniquely sensitive because "[a] cell phone faithfully follows its owner . . . into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218. For that reason, the Court concluded that CSLI searches "present[] even greater privacy concerns than the GPS monitoring of a vehicle." *Id*. Finally, "the retrospective quality of [CSLI] gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's

whereabouts, subject only to the retention policies of the wireless carriers," which can date back years. *Id*. at 2218.

In short, there has never been a more invasive way for law enforcement to search and surveil than there is today through cell phone and CSLI searches. This is precisely what led the U.S. Supreme Court to chart a new course in Fourth Amendment jurisprudence and afford special protections to cell phone and CSLI records. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2214 ("[A] central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'") (quoting *United States v. Di Re*, 332 U.S. 581, 68 S. Ct. 222, 92 L. Ed. 210 (1948)); Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (last revised Dec. 29, 2018) (Oxford Univ. Press, forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 (arguing that "new rules are needed to restore the role of the Fourth Amendment" and that "[t]he Supreme Court has already begun creating a Digital Fourth Amendment in *Carpenter* and . . . in *Riley v. California*").

II. It is already well established that a search of cell phone and CSLI records must be supported by probable cause to believe that evidence of a crime will be found in those particular records.

The Court of Appeals correctly held that the search warrant application at issue here was deficient under existing law because the nexus requirement was unmet. It is already well established that a search of cell phone and CSLI records must be supported by probable cause to believe that evidence of the crime under investigation will be found in those specific

records; and the briefs submitted by Mr. Denham accurately characterizes the law under the Washington Constitution on this point. Namely, Mr. Denham correctly points out that this Court has consistently "rejected a 'per se' rule that once a person is suspected of criminal activity, a finding of probable cause to search a particular location automatically follows." Suppl. Br. of Resp. at 12. Instead, this Court has consistently demanded "a nexus between criminal activity and the item to be seized." *State v. Thein*, 138 Wn.2d 133, 140, 977 P.2d 582 (1999). This Court has thus found constitutional violations where search warrants issued based on generalized statements that drug dealers tend to keep drugs and paraphernalia in their homes, and that homicide perpetrators tend to return to a scene of the crime. *See id.*; *State v. Jackson*, 150 Wn.2d 251, 76 P.3d 217 (2003). Mr. Denham has also pinpointed cases where the Court of Appeal has demanded a sufficient nexus in cases where law enforcement sought to conduct electronic searches—of cell phones or computers—based on blanket statements of habits of gang members and sex offenders. *See* Suppl. Br. of Resp. at 12-13 (describing *State v. Keodara*, 191 Wn. App. 305, 315, 364 P.3d 777 (2015), and *State v. Nordlund*, 113 Wn. App. 171, 182, 53 P.3d 520 (2002)).

The Court of Appeal got it right here: The Washington Constitution does not allow law enforcement to search cell phones or CSLI records based on broad generalizations of what suspected burglars tend to do; much less what *all* innocent Americans tend to do. *See* CP 424 (affidavit requesting warrant based on proposition that "the majority of Americans possess and

use cellular telephones, and that most of those keep the phones within their reach at all times").

Amici write separately to point out that many *federal* courts have recognized that the Fourth Amendment, which is less protective than article 1, section 7 of the Washington Constitution, also recognizes the importance of the nexus requirement when it comes to cell phone and CSLI searches. For example, in *United States v. Ramirez*, 180 F. Supp. 3d 491 (W.D. Ky. 2016), the court suppressed evidence seized from a cell phone because "there [was] nothing in the [warrant] affidavit asserting that [Detective] Petter knew [Defendant] Ramirez used the phone as a tool of drug trafficking." *Id*. at 496. The court instead observed that "[t]he only information in the [warrant] affidavit indicating any likelihood that evidence of a crime might be found on Ramirez's phone was the fact that he was arrested for an alleged drug conspiracy while he possessed the phone." *Id*. at 495. But the court found this insufficient under the Fourth Amendment, because "[p]ossessing a cell phone during one's arrest for a drug-related conspiracy is insufficient by itself to establish a nexus between the cell phone and any alleged drug activity." *Id*. And in *United States v. Lyles*, 910 F.3d 787 (4th Cir. 2018), the Fourth Circuit brusquely rebuked law enforcement for seeking to search cell phones located inside a home based on nothing more than the fact that marijuana stems were found in a trash can outside the home. *Id*. at 795 ("[T]he warrant application lacked any nexus between cell phones and marijuana possession. There is insufficient reason to believe that any cell phone in the home, no matter who

owns it, will reveal evidence pertinent to marijuana possession simply because three marijuana stems were found in a nearby trash bag."). Decisions on the other side of the issue, where courts have found a sufficient nexus to justify cell phone or CSLI searches, are equally cognizant of the importance of that requirement. *See, e.g.*, *United States v. Merriweather*, 728 F. App'x 498, 506 (6th Cir. 2018) (unpublished) (finding sufficient nexus where affidavit "allege[d] that cell phones were used to facilitate two drugs buys from [the defendant and] . . . the particular cell phone at issue was found in a vehicle containing apparent oxymorphone, the very drugs involved in the conspiracy"); *United States v. Bass*, 785 F.3d 1043, 1049 (6th Cir. 2015) (finding sufficient nexus where the affidavit stated that the *particular* defendant "and his co-conspirators [in an identity-theft investigation] frequently used cell phones to communicate" and the affiant believed the cell phone at issue was possibly being used by the defendant to "alert other conspirators of [his] arrest . . . after he was notified of the Arrest Warrant").

The rationale of these federal cases applying Fourth Amendment law further support the decision by the Court of Appeal here, because "[i]t is well established that article I, section 7 is qualitatively different from the Fourth Amendment and provides *greater* protections." *State v. Hinton*, 179 Wn.2d 862, 868, 319 P.3d 9 (2014) (en banc) (emphasis added). This Court should thus affirm the Court of Appeal's decision and make clear to other courts that warrant applicants must explain—through case-specific facts, as opposed to generalized statements—why a search of particular cell phone

or CSLI records will likely uncover evidence of the specific crime under investigation.

III. This Court should hold that Washington law further demands "scrupulous exactitude" when a warrant seeks cell phone or CSLI records.

The Court of Appeals thus offered a routine application of the nexus requirement to the facts of Mr. Denham's case. But this Court should not simply reiterate existing law. Instead, it should clarify that a heightened standard applies when law enforcement seeks to search cell phone or CSLI records because such records implicate the First Amendment.

"The First Amendment imposes special constraints on searches for and seizures of presumptively protected material, and requires that the Fourth Amendment [and the more protective analogue in the Washington Constitution] be applied with 'scrupulous exactitude' in such circumstances." *Maryland v. Macon*, 472 U.S. 463, 468, 105 S. Ct. 2778, 86 L. Ed. 2d 370 (1985) (citations omitted); *see also State v. Perrone*, 119 Wn.2d 538, 547, 834 P.2d 611 (1992) ("Where a search warrant authorizing a search for materials protected by the First Amendment is concerned, the degree of particularity demanded is greater than in the case where the materials sought are not protected by the First Amendment."). Certain kinds of materials are presumptively subject to First Amendment protection and thus the "scrupulous exactitude" standard—including "Books, films, and the like . . . where their content is the basis for seizure." *Perrone*, 119 Wn.2d at 550. Amici respectfully urge this Court to add cell phone and CSLI records to this list, and to hold that such searches can only occur pursuant

to the scrupulous exactitude standard because they tend to contain expressive materials and reveal associational activity.

At least two appellate courts in Washington have already recognized that "because [cell phones] are repositories for expressive materials protected by the First Amendment, the Fourth Amendment's particularity requirement is of heightened importance in the cell phone context." *Fairley*, 12 Wn. App. 2d at 320; *State v. McKee*, 3 Wn. App. 2d 11, 413 P.3d 1049 (2018), (citing "scrupulous exactitude" standard in case involving cell phone search), *rev'd and remanded on other grounds*,[4] 193 Wn.2d 271, 438 P.3d 528 (2019).[5]

First, in *Fairley*, law enforcement obtained a warrant authorizing them to search an individual's residence and his car, and to *seize* certain listed property found at these locations—including a cell phone. Law enforcement insisted that the authorization to seize the cell phone included authorization to search the cell phone, but the Court of Appeal quickly rejected that argument. The court observed that "[t]he Washington constitution provides broader protection" than the Fourth Amendment, and that law enforcement's argument ignored the particularity requirement, which, under both the state and federal constitution, requires "[n]arrow

[4] This Court reversed only the *remedy* portion of *McKee*. The Court of Appeals had ordered certain counts dismissed due to the deficiency of the search warrant, but this Court held that the proper remedy was instead to suppress the cell phone evidence. This Court did not disapprove of the underlying analysis regarding the warrant deficiency.
[5] *See also Rouzan v. Dorta*, No. EDCV 12-1361, 2014 WL 1716094, at *9 (C.D. Cal. Mar. 12, 2014), *report and recommendation adopted*, 2014 WL 1725783 (C.D. Cal. May 1, 2014) (federal case noting "that the seizure and search of Plaintiff's cellphone are assessed under the heightened protection afforded First Amendment materials").

tailoring" to prevent "'overseizure and oversearching' beyond the warrant's probable cause authorization." *Id*. at 320 n.3, 321. It also noted that, as a general matter, "a search warrant allowing for a 'top-to-bottom search' of a cell phone" would lack particularity and narrow tailoring and thus fail to meet the particularity requirement. *Id*. at 322. Instead, the court explained that:

> [T]he Fourth Amendment demands a cell phone warrant specify the types of data to be seized with sufficient detail to distinguish material for which there is probable cause from information that should remain private. For example, in addition to identifying the crime under investigation, the warrant might restrict the scope of the search to specific areas of the phone (e.g., applications pertaining to the phone, photos, or text messages), content (e.g., outgoing call numbers, photos of the target and suspected criminal associates, or text messages between the target and suspected associates) and time frame (e.g. materials created or received within 24 hours of the crime under investigation). It might also require compliance with a search protocol, designed to minimize intrusion into personal data irrelevant to the crime under investigation.

Id. at 322-23. (citations omitted). The court then went further, and described key First Amendment concerns as well: explaining that "[a] cell phone provides access to a vast amount of material protected by the First Amendment," and that "[a] cell phone data search can reveal a user's travel history, weight loss goals, religious beliefs, political affiliations, financial investments, shopping habits, romantic interests, medical diagnoses, and on and on." *Id*. at 323.

The second, more fact-intensive analysis of the heightened importance of particularity in the cell phone context was in *McKee*. In that case, a mother discovered that a drug dealer had used his cell phone to take photos and videos of her minor daughter engaged in sexual acts. The mother delivered this cell phone to law enforcement and explained that she had seen these photos and videos on the cell phone. Law enforcement then applied for a warrant to search the cell phone, but the resulting warrant broadly authorized seizure of: "Images, video, documents, text messages, contacts, audio recordings, call logs, calendars, notes, tasks, data/[I]nternet usage, any and all identifying data, and any other electronic data from the cell phone showing evidence of the above listed crimes." 3 Wn. App. 2d at 18.

When asked to pass upon the warrant, the Court of Appeal started by noting how "[t]he advent of . . . cell phones that store vast amounts of personal information makes the particularity requirement of the Fourth Amendment that much more important," and thus cited the "scrupulous exactitude" standard before considering its constitutionality. *Id*. at 24-25. The court then held that the warrant failed to pass muster. The court explained that "above list of crimes" limiting language was ineffective because that list did not include the statutory language defining the crimes of sexual exploitation of a minor and dealing in depictions of a minor engaged in sexually explicit conduct; and, as a result, the warrant was rendered "overbroad and allowed the police to search and seize lawful data when the warrant could have been made more particular." *Id*. at 26. Indeed, the search warrant could have easily been made more particular if it would

have included or incorporated additional information that had been included in the supporting affidavit—like the relevant time frames in which the specific video clips and photographs would be found. *Id*. at 28.

The rationale of *Fairley* and *McKee* is sound and justifies a clear holding from this Court imposing presumptive First Amendment protections on cell phone records. That presumption should also apply to CSLI held by third parties, because the First Amendment concerns—specifically, the freedom of association concerns—are no less significant in that context. *See Muhammad*, 194 Wn.2d at 589 (recognizing that a detailed record of "public movements[] can expose personal details about family, politics, religion, and sexual associations") (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)). As this Court noted nearly two decades ago, a GPS device attached to a vehicle "can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the 'wrong' side of town, the family planning clinic, the labor rally . . . [and] can reveal preferences, alignments, associations, personal ails and foibles." *Jackson*, 150 Wn.2d at 262. These associational concerns become more acute in the CSLI context because, as the U.S. Supreme Court noted in *Carpenter*, cell phones can go places that vehicles cannot. *See Carpenter*, 138 S. Ct. at 2218.

Here, the scrupulous exactitude standard is unmet with respect to the CSLI at issue on appeal because the search warrant addendum authorized seizure of all location data from "11/11/2016 though [April 20, 2017]" because these records "would assist in providing information on [Mr. Denham's] location during the above listed crimes," i.e., during the burglary and theft and trafficking in stolen property. Pet., App. C, Warrant Aff. at 4, 8 & 9. But this effectively authorized retroactive, 24-hour location surveillance of Mr. Denham for five *months* even though there is no reason to believe that *all* of Mr. Denham's movements over those five months were relevant to the crimes under investigation. Indeed, the affidavit instead suggested that the only relevant dates would be November 11, 2016 (the night of the burglary and theft), January 26, 2017 (when Mr. Denham allegedly pawned a necklace at a shop in Bellevue), and March 21, 2017 (when Mr. Denham returned to the same shop to attempt to pawn 4-5 diamond gold rings). Pet., App. C, Warrant Aff. at 4. The warrant was thus far from scrupulously exact because it sought CSLI for all dates over a five-month period, despite the comparatively narrow reasons proffered for the search.

IV. This case highlights the importance of providing courts with clear guidance to ensure meaningful privacy protections.

Article I, section 7 of the Washington Constitution "is qualitatively different from the Fourth Amendment and provides greater protections." *Hinton*, 179 Wn.2d at 68 (discussing Wash. Const. art. I, § 7). And, as noted above, searches of cell phone and CSLI records raise First Amendment

concerns that require searches to satisfy the scrupulous exactitude standard. To ensure meaningful privacy protection in a manner that satisfies article I, section 7, of the Washington Constitution, the Court could—in an appropriate case—consider articulating clear standards or requirements for warrants authorizing searches of cell phone or CSLI records. *See, e.g.*, *Fairley*, 12 Wn. App. 2d at 322 (noting that a warrant to search a cell phone may "require compliance with a search protocol, designed to minimize intrusion into personal data irrelevant to the crime under investigation" in order to satisfy Washington law and the First Amendment.)

For example, the Court could require independent review teams to ensure that a search warrant does not give law enforcement access to irrelevant records that document the personal activities of the target. *See, e.g.*, *State v. Mansor*, 363 Or. 185, 220-21, 421 P.3d 323 (2018) (recognizing that "[e]ven a reasonable search authorized by a valid warrant necessarily may require examination of at least some information that is beyond the scope of the warrant" and holding that internet searches from a time period for which there was no probable cause to search must be suppressed absent an applicable warrant exception). Or the Court could require a robust, court-approved search protocol or displacement of the plain view doctrine—as described in a concurring opinion authored by the then-Chief Judge of the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.* (hereinafter "*CDT Testing*"), 621 F.3d 1162, 1179 (9th Cir. 2010). Such tools can be used to prevent "general, exploratory rummaging in a person's belongings," *McKee*, 3 Wn. App. 2d at 21 (quoting

Andresen v. Maryland, 427 U.S. 463, 480, 96 S. Ct. 2737, 49 L. Ed. 2d 627 (1976)), and are also flexible enough to be tailored in ways most appropriate for the individual case at hand. *See, e.g.*, *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 168 (D.D.C. 2014) ("The Court is not dictating that particular terms or search methods should be used. Instead, the Court is attempting to convey that it wants a sophisticated technical explanation of how the government intends to conduct the search so that the Court may conclude that the Government is making a genuine effort to limit itself to a particularized search."). These are thus powerful mechanisms that could be deployed by Washington courts to mitigate, and potentially eliminate, the intrinsic and otherwise unavoidable privacy concerns raised by searches of cell phone and CSLI records.

* * *

The recent, near-universal adoption of the cell phone has led to a "Golden Age of Surveillance," in which law enforcement can now tap into neatly compiled troves of personal information. *Going Dark: Encryption, Tech., and the Balance Between Public Safety and Privacy: Hearing Before the S. Judiciary Comm.*, 114th CONG. (2015) (statement of Peter Swire, Huang Professor of Law & Ethics, Scheller College of Business, Georgia Institute of Technology), https://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf. Accordingly, although law enforcement might argue against the heightened standards articulated above, any administrative burdens caused by application of the scrupulous

exactitude standard are "more than offset by [the] massive gains" offered by cell phone and CSLI records that *can still* be obtained subject to those safeguards. *Id*. Indeed, it is precisely because cell phone and CSLI records offer such effective tools—tools that were unfathomable when the Fourth Amendment was drafted—that the courts must step in "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (quoting *Di Re*, 332 U.S. at 581); *see also* Kerr, *supra*, at 2 (arguing that the Supreme Court recognized and acted upon the need for equilibrium adjustment in *Carpenter* and *Riley*).

CONCLUSION

For the reasons stated above, Amici respectfully ask the Court to affirm the Court of Appeal's holding that Washington law does not allow law enforcement to search cell phones or CSLI records based on broad generalizations of what suspected burglars tend to do or what all innocent Americans tend to do, and to hold that the "scrupulous exactitude" standard applies when a warrant seeks cell phone or CSLI records.

RESPECTFULLY SUBMITTED this 7th day of December, 2020.

PERKINS COIE LLP

By: */s/ John R Tyler*
John R. Tyler, WSBA #42097
Anna Mouw Thompson, WSBA #52418
Rachel Dallal, WSBA #88558
Counsel for Amicus Curiae WACDL

WACDL AMICUS COMMITTEE
Mark B. Middaugh, WSBA #51425

ACLU OF WASHINGTON FOUNDATION
Antoinette M. Davis, WSBA #29821
Nancy Talner, WSBA #11196

KING COUNTY DEPARTMENT OF PUBLIC DEFENSE
La Rond Baker, WSBA #43610
Katie Hurley, WSBA #37863
Brian Flaherty, WSBA #41198

WASHINGTON DEFENDER ASSOCIATION
Alexandria "Ali" Hohman, WSBA #44104

CERTIFICATE OF SERVICE

Today I caused to be filed, electronically, the foregoing document via the Washington State Appellate Courts' Secure Portal, which will automatically cause such filing to be served on counsel for all other parties in this matter via the Court's e-filing platform.

I certify under penalty of perjury under the laws of the State of Washington that the foregoing is true and correct.

DATED: December 7, 2020, at Seattle, Washington.

June Starr
June Starr

PERKINS COIE LLP

December 07, 2020 - 4:46 PM

Transmittal Information

Filed with Court:	Supreme Court
Appellate Court Case Number:	98591-0
Appellate Court Case Title:	State of Washington v. Lynell Avery Denham

The following documents have been uploaded:

- 985910_Briefs_20201207163423SC797950_5784.pdf
  This File Contains:
  Briefs - Amicus Curiae
  The Original File Name was 2020-12-07 Amicus Brief.pdf
- 985910_Motion_20201207163423SC797950_1332.pdf
  This File Contains:
  Motion 1 - Amicus Curiae Brief
  The Original File Name was 2020-12-07 Motion for Leave to File Amicus Brief.pdf

A copy of the uploaded files will be sent to:

- Sloanej@nwattorney.net
- athompson@perkinscoie.com
- dennis.mccurdy@kingcounty.gov
- jstarr@perkinscoie.com
- kochd@nwattorney.net
- paoappellateunitmail@kingcounty.gov
- rdallal@perkinscoie.com
- swiftm@nwattorney.net

Comments:

1. Motion for Leave to File Brief of Amici Curiae 2. Brief of Amici Curiae

---

Sender Name: John Tyler - Email: RTyler@perkinscoie.com
Address:
1201 3RD AVE STE 4900
SEATTLE, WA, 98101-3099
Phone: 206-359-3034

Note: The Filing Id is 20201207163423SC797950